

IN THE CLAIMS

Please amend the claims as indicated:

1. (currently amended) A service for managing a secure network boot of a server blade, the server blade being in a blade chassis that has multiple server blades, the blade chassis including a switching means allowing the server blade to communicate with a network, the service comprising:

storing a list of trusted management servers in a management module on a server blade;

broadcasting a Dynamic Host Configuration Protocol (DHCP) DISCOVER request to a network of DHCP servers;

~~broadcasting a request for a boot program from a server blade to a network of management servers;~~

receiving, at a switching means associated with the server blade, a DHCP OFFER message that is responsive to the DHCP DISCOVER request, wherein the DHCP OFFER message contains Internet Protocol (IP) addresses of responding DHCP servers, a Dynamic IP address with lease information, and a list of Pre-boot eXecution Environment (PXE) Boot Servers that can be contacted by the server blade to download a boot program, and wherein the DHCP OFFER comes from a responding DHCP server on the network of DHCP servers;

~~receiving a response to the request for the boot program at a switching means associated with the server blade, the response being from a responding management server on the network of management servers, the response containing directions to a boot program server;~~

comparing an identity of the responding [[management]] DHCP server with the list of trusted [[management]] DHCP servers in the management module on the server blade;

[[upon]] in response to verifying that the responding [[management]] DHCP server is on the list of trusted [[management]] DHCP servers, transmitting the response from the responding management server to the server blade permitting the DHCP OFFER message to pass through to the server blade via an Ethernet switch that is coupled to the server blade, and downloading a boot program from a boot program server specified by the responding [[management]] DHCP server;

[[upon]] in response to determining that the responding [[management]] DHCP server is not on the list of trusted [[management]] DHCP servers, blocking the transmittal of the response from the responding [[management]] DHCP server through the Ethernet switch to the server blade; and

[[upon]] in response to determining that the responding [[management]] DHCP server is not on the list of trusted [[management]] DHCP servers, generating an alert to a designated administrator server of a presence of an unauthorized [[management]] DHCP server on the network of [[management]] DHCP servers.

2. (original) The service of claim 1, further comprising:

coordinating different types of boot program servers available to the server blade by maintaining, in an information technology services organization logically oriented between the different types of boot program servers and the server blade, a permission list of boot program servers authorized for each server blade in a server blade chassis.

3. (new) The service of claim 2, wherein the information technology services organization is an Information Technology (IT) services organization that manages various types of Pre-boot eXecution Environment (PXE) deployment servers; and wherein the IT services organization enables a same IT service organization assigned systems administrator to manage the various types of PXE deployment servers, to maintain permission lists for each PXE server type, to monitor a network for a presence of unauthorized PXE servers that are not authorized, by the IT services organization, to support the client computer, and to shut down network ports, for unauthorized PXE servers, in the client computer.

4. (new) The service of claim 1, wherein the alert to the designated administrator server is made using a Simple Network Management Protocol (SNMP) trap sent by the server blade.

5. (new) The service of claim 1, wherein none of the steps described in claim 1 causes any code changes to firmware in the server blade.

6. (new) The service of claim 1, further comprising:

in response to the responding DHCP server not being on the list of trusted DHCP servers,  
downloading a boot program fro a trusted PXE server on a secure Local Area Network (LAN).